L-26: Safeguarding Protected Information

POLICY: See L-26 Safeguarding Protected Information at www.cosdcompliance.org.

DEFINITIONS: See HHSA Policy L-30 Privacy Definitions.

PROCEDURES:

A. Workspace and Desks:
   1. Ensure Protected Information (PI) is attended to at all times. Always lock (Ctrl-Alt-Del-Enter) your computer and keep paper documents out of sight when not in use.
   2. At the end of each day:
      a. Check that your desk is clear and your confidential shred bin is empty;
      b. Secure any paper documents containing PI and County assets (like a laptop, tablet, smartphone, or flash drive) in a locked filing cabinet, with a cable lock, or locked workspace within a locked office (two layers of security).

B. Printers, Copiers, and Faxes:
   1. Pick up printed documents containing PI promptly from the printer or fax and ensure you only take what belongs to you;
   2. Ensure printers, copiers, and faxes that produce PI are kept in secured areas;
   3. Only make a scan, copy, and print PI on County-approved copy machines;
   4. For BHS and Eligibility Program faxes: Program staff must contact the fax recipient to verify the fax number and receipt.

C. Conference and Interview Rooms:
   1. Be mindful of who can see PI you display on a whiteboard, flip chart, or projector screen;
   2. Ensure no PI is left on the conference table or a board after a meeting;
   3. For BHS/Eligibility Programs: Escort all visitors through areas containing PI.

D. Emails:
   1. Ensure any PI you send outside of the County network is encrypted;
   2. Never send work-related emails to your personal email account;
   3. Be mindful when replying to or forwarding emails containing PI. You are responsible for the entire thread, not just what you type.

E. Handling and Storing PI:
   1. PI must only be stored on County-approved, encrypted devices and never on a personal device;
   2. Make sure that PI is shared with the correct individuals;
      a. Verify email recipients before you hit 'send;'
      b. Ensure you have adequately identified clients before providing them PI;
      c. Update client addresses promptly and accurately;
   3. Ensure PI is secured and not left in areas available to the public, clients, or facility visitors.

F. Phones:
1. Contact County clients using County phones only. Never provide your personal phone number to clients;
2. Never take pictures of clients or PI using a personal phone;
3. Be mindful of any PI you leave on an answering machine;
4. Verify the identity of callers before sharing PI on the phone.

G. Social Media:
1. Never post PI on social media accounts.

H. Leaving the Office:
1. Obtain permission from your supervisor before removing PI from a County facility. Staff removing PI from a County facility must first complete HHSA Form 23-26;
2. Keep paper documents that contain PI and all County assets (such as laptops, tablets, smartphones, and flash drives) with you at all times;
    a. When at home, ensure paper PI and assets are in a safe, secure location;
    b. No PI should ever be left in a car overnight. For BHS and Eligibility Programs, PI should never be left unattended in a car or the trunk not even for a few minutes. For BHS and Eligibility Programs, PI may also never be checked on an airplane.

I. Tracking Assets:
1. Programs must maintain a current inventory of all County assets, such as desktops, laptops, tablets, smartphones, and flash drives;
2. Any loss or theft of a County asset shall be immediately reported to the Agency Privacy Officer by email.

J. Disposing of PI:
1. Papers containing PI shall be shredded using an Agency Privacy Officer approved shredder or Countywide shredding company;
2. For information on how to dispose of County electronic assets, consult Agency IT.

K. Teleworking:

When accessing County Protected Information (PI) while working remotely.

1. Remote Access:
    a. Use only County-approved VPN solutions.
    b. Use a non-public WiFi connection.

2. Personal Printer:
    a. Obtain prior approval from the supervisor before printing any documents containing any County PI while teleworking.
    b. Only print County PI that is absolutely needed and is the minimum necessary.
    c. Do not use printing services at a UPS or FedEx or other similar copy shops.
    d. Do not use a friend or neighbor's printer; only use printers within your own residence.
    e. Promptly delete the files from the personal printer's hard drive. Directions to complete this step can be found in printer user manuals.

3. Remotely Handling and Storing PI:
    a. Keep paper documents in a locked drawer/cabinet when not in use.
        - Never leave unattended in any location for any length of time (including vehicles).
    b. Save electronic files only on County-approved, encrypted devices and never on a personal device.
    c. Return paper documents containing PI to a County location for filing or disposal; Do not dispose the documents while teleworking nor use a personal shredder or other shredding and document destruction services.

4. Workstation:
    a. Use a privacy screen or position the monitor(s) from being viewable by others.
    b. Lock your computer each time when you walk away.
    c. Restrict access to the device from other household members.

5. Telehealth and Video Conferencing:
    a. Ensure you conduct meetings and conversations that may include PI in a private location so that others cannot overhear.
    b. Use only County approved platforms, such as MS Teams Meeting and WebEx. All other platforms require prior approval from the Agency Compliance Office.
    c. Restrict the sharing of documents containing PI to County approved file-sharing storage platforms (e.g., SharePoint, S:\Dr, OneDrive), not as a part of the meeting itself.

QUESTIONS/INFORMATION: HHSA Privacy Officer at 619-338-2808